聚焦安全：用SSLVPN设备简化安全访问 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E8_81_9A_E7_84_A6_E5_AE_89_E5_c101_142688.htm 许多公司使用VPN向公司外部的员工提供企业网络接入。目前，大多数远程接入VPN都使用IP安全扩展(IPsec)加密在公共IP网络上传输的专用IP数据包。然而，随着员工队伍的增长和多元化，IPsec VPN客户对于最终用户来说是很麻烦的，对于网络管理员来说是成本是很高的。通过利用广泛应用的网络浏览器作为一个客户平台，SSL VPN设备将是提供一种简单而安全的外点访问专用企业服务和数据的有希望的替代方法。 为什么使用SSL VPN设备? 市场研究公司Gartner预测，到2008年，SSL VPN将成为主要的远程接入方式。三分之二以上的远程工作员工、四分之三的承包商和90%以上的需要随机访问企业网络的雇员都将采用这种方式。作为一个基于浏览器的解决方案，SSL VPN几乎能在任何系统上快速启动，不需要安装永久性的客户端软件。对于那些对管理旅行者和远程工作者的笔记本电脑感到厌烦以及那些需要不增加已经很沉重的IT工作量来扩大远程接入的企业来说，上述好处是有吸引力的。用户通常可以使用一台SSL VPN设备从家里的或者公共的PC上加入网络，在任何可用的互联网连接上获得直接的访问。一旦用户通过身份识别，组或者单个规则便允许访问SSL VPN设备后面的代表系统、服务和数据的URL。目标应用一般通过一个浏览器的窗口显示出来，由下载的ActiveX控件或者Java程序实施的。SSL 或者其IETF(互联网工程任务组)的继任者TLS(传输层安全)将用于数据压缩、散列、加密和在用户

和VPN设备之间的传输全部信息。总之，SSL VPN设备能够提供安全的访问，较少地依赖客户端软件。 应用SSL VPN设备 深入挖掘这个漂亮的外表，你将会发现SSL和IPsec VPN之间的巨大差别。例如，IPsec VPN提供访问具体的子网或者整个企业网络。连接的主机必须分配一个这个专用网络地址空间中的IP地址。因为SSL VPN提供具体URL地址的访问，资源规则可以更详细并且能过更容易地隐藏内部网络的结构。从网络工程师的观点看，SSL VPN整合更简单，因为这种设备能够在你防火墙的隔离区中使用，不用增加IP子网或者重新为IP子网编号。 另一方面，IPsec VPN创建一个支持任何基于IP的应用程序的强大的、通用的应用程序。根据其设计，SSL VPN设备可能需要逐步努力支持新的应用。例如，详细的设置可能需要把URL镜像为应用对象，并且重写URL以便隐藏内部信息。每一个SSL VPN设备都支持通用商务应用程序，如企业电子邮件和网络文件系统访问等。但是，专有的或者复杂的应用需要客户介入开发或者需要客户方面的端口转发代码。因此，许多公司最初都使用SSL VPN来增强其IPsec VPN，把仅需要访问电子邮件的员工增加到SSL VPN网络，同时保留IPsec VPN以满足真正需要广泛的网络层访问的员工的需求。 在SSL VPN设备中寻求什么 当然，SSL VPN设备必须有增强的平台的操作系统，并且通过安全界面进行管理。虽然早期的SSL VPN性能与IPsec相比还不是很好，但是，目前的企业设备能够使用硬件加速和高可用性等技术可靠地支持每一个大型的员工队伍。但是，除了对任何网络安全设备的这些基本的考虑之外，当你选择一台SSL VPN设备的时候，你应该考虑什么功能和因素呢? VPN架构SSL VPN设

备是多种多样的： Web代理设备仅支持Web应用程序。浏览器把普通的HTTP包在SSL中并且发送给这台设备。这台设备检查政策、镜像URL并且把HTTP请求转发给目标互联网服务器。 应用解析设备让用户通过ActiveX或者Java接口与应用程序互动。这种Java接口模仿本地的应用程序图形用户界面，但是以HTTP格式发送请求。这台设备在把这个请求转发到目标服务器(非Web服务器)之前必须要把HTTP解析为每一个应用程序的本地协议。 端口转发设备通过使用一个客户端代理在SSL隧道中转发本地应用协议来支持TCP客户机/服务器应用程序。这个代理与远程主机的应用端口连接在一起，同时，这台设备转发内部服务器(非Web服务器)发出和接收的信息。网络扩展设备通过使用一个客户端代理在一个SSL隧道中转发IP数据来支持任何IP应用程序。一个安装的代理拦截并且把出网的IP数据传送给这个设备。这台设备像一台网络层网关一样工作，在结构上与IPsec相似，但是没有标准IPsec的限制。 任何指定的设备可能都支持一个以上的结构。但是，从这里开始，将帮助你理解产品的客户和应用程序支持。 客户支持：每一个SSL VPN使用Web浏览器当作一个客户平台。但是，许多下载的客户端代码限制在公共PC、非Windows主机、移动设备以及外部网合作伙伴的系统上使用。你能够满足客户的要求吗，例如客户对浏览器厂商/版本或者启用ActiveX的要求?这种设备能为现值的客户提供减少的功能，同时为使用VPN门户网页自己安装代理软件的雇员提供更多的功能吗?应用程序支持：除了电子邮件和文件共享之外，考虑你的员工队伍需要的应用程序，这种设备是否/如何支持这些应用程序以及实现这些应用所需要的努力。例如，端口转发设备通

常不需要客户化就能够支持许多客户机/服务器。但是，实时的应用(如VoIP)可能需要网络扩展设备。确认你理解了在URL镜像和为你需要的应用程序进行协议解析都涉及到什么。 用户身份识别：SSL VPN在提供授权服务之前必须要识别用户的身份。确认这种设备支持你需要的用户身份识别方式以及现有的身份识别服务器和用户数据库(如, RADIUS、主动目录和LDAP)。此外，你要考虑这种设备是否能够从用户账户提取授权属性，并且考虑建立这种工作流所涉及的整合努力。 授权：SSL VPN通常有能力强制执行控制用户(或者组)能够访问什么内容的详细规则。评估支持每一个需要的应用程序/资源的授权详细规则，苹果这种设备是否支持你定义的安全政策。例如，一些SSL VPN能够识别远程设备身份，让你限制那些在公共或者家庭PC上的用户的功能。 端点安全：在批准访问之前评估端点安全状况和一台设备的状况也是很有用的。SSL VPN支持是为NAC、NAP、TNC和产品具体界面开发的，使它能够检查和/或者强制执行端点安全。采取的方法是要求在端点使用当前的安全补丁或者杀毒软件，或者限制不符合规定的端点能够访问的资源。考虑这种设备如何更好地适应你们公司的端点安全战略和实施。如果你计划支持没有管理的端点，你要评估对客户端安全措施的支持，如浏览器缓存、cookie和历史记录的清除以及"沙盒处理"(sandboxing)。 